NASA Contractor Report 181850

ASSESSMENT TEAM REPORT ON FLIGHT-CRITICAL SYSTEMS RESEARCH AT NASA LANGLEY RESEARCH CENTER

[redacted]

Daniel P. Siewiorek and Janet R. Dunham, Compilers

Center for Digital Systems Research
Research Triangle Institute
Research Triangle Park, N. C. 27709

P71

Contract NAS1-17964
Task Assignment No. 29
August 1989

NOTICE

Date for general release August 31, 1991

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23665-5225

ASSESSMENT TEAM REPORT ON FLIGHT-CRITICAL SYSTEMS RESEARCH AT NASA LANGLEY RESEARCH CENTER

ASSESSMENT TEAM MEMBERS:

Daniel P. Siewiorek, Chairman
Cary R. Spitzer, NASA Representative
Janet R. Dunham, Coordinator
Greg Chisholm
Eliezer G. Gai
John E. Reed
Peter J. Saraceni
Herman Schmid
Anthony S. Wojcik

Contents

EXECUTIVE SUMMARY

In November 1988, an Assessment Team was formed to assist NASA Langley Research Center (NASA Langley) in assessing the quality, coverage, and distribution of effort of the flight-critical systems research program at NASA Langley. This program spans several branches in the Information Systems Division at NASA Langley, with the bulk of the research being conducted by the System Validation Methods Branch. The Assessment Team had two primary sources of information on the research program: (1) review of the NASA Langley flight-critical systems research program by attending a one-day briefing at NASA Langley and reviewing representative research publications and (2) participation at the Flight-Critical Digital Systems Technology Workshop held at NASA Langley on December 13-15, 1988. Immediately after the workshop, the Assessment Team held a meeting to determine the key recommendations set forth in this report.

Within the scope of the review, the Assessment Team has found the research program to be very sound. All tasks under the current research program are at least partially addressing the industry needs. However, the workshop generated many more critical research needs than the Information Systems Division has resources. The Assessment Team recommends that the program resources be substantially expanded to give adequate coverage to the existing research and extended to the additional industry needs identified. Specifically, the Assessment Team's consensus is that the following three recommendations be emphasized in any ensuing action. First, the current program should be extended to include research and development in operations and maintenance. Second, the five highest priority research needs should receive additional funding. These needs are:

1. the development of a validated hierarchical integrated tool set that can be used to address issues related to life-cycle validation

2. the conduct of cost-tradeoff and effectiveness studies of design methodologies and fault tolerance concepts

3. the development and verification of easy-to-use modeling tools that address reliability, performance, coverage, and cost

4. the conduct of threat modeling, and propagation analysis and testing. In particular, develop design verification criteria for Electromagnetic

Environment(EME)and High Energy Radio Frequency (HERF) related threats.

5. the compilation and analysis of in-service data

Third, the research program should be focused by selecting an actual hardware and software system that is under development as a vehicle for the on-going evaluation of emerging technology.

These recommendations are made in conjunction with the suggestion that an overall strategy be followed. This strategy involves NASA, the aerospace industry, and the FAA cooperating in the development of an integrated methodology for design, verification, and validation of flight-critical systems that are key to U.S. leadership in the next century. The automotive and electronics industries in the U.S. have lost their competitiveness to stronger foreign corporations. Industry data is beginning to suggest a similar threat to the U.S. aerospace industry, especially aviation. Through NASA, the aerospace industry, and FAA cooperating, there is an opportunity to address this threat before it is too late. A relevant precedence for this suggestion is in the information processing industry. Organizations like the Micro-electronics Computing Consortium (MCC) and the Software Productivity Consortium have been formed by cooperating agencies in order to develop a competitive edge.

1 Introduction and Overview

1.1 The Assessment Team

The Assessment Team evaluated the quality, coverage, and distribution of effort of the flight-critical digital systems research program in the Information Systems Division at NASA Langley Research Center. The team was composed of:

- Dr. Daniel P. Siewiorek, Chairman
  Carnegie-Mellon University
- Mr. Cary R. Spitzer, NASA Representative
  NASA Langley Research Center
- Ms. Janet R. Dunham, Coordinator
  Research Triangle Institute
- Mr. Greg Chisholm
  Argonne National Laboratory
- Dr. Eliezer G. Gai
  The Charles Stark Draper Laboratory, Inc.
- Mr. John E. Reed
  Mr. Peter J. Saraceni
  FAA Technical Center
- Mr. Herman Schmid
  General Electric Company
- Dr. Anthony S. Wojcik
  Michigan State University

1.2 Assessment Team Activities

1.2.1 Research Briefing

The Assessment Team members attended a one-day briefing on the flight-critical digital systems research program at NASA Langley. Appendix A provides the agenda for this briefing. This briefing informed the Assessment Team on flight-critical digital systems research activities at NASA Langley in a format that allowed interaction with the researchers. The Assessment Team was also provided with extensive publications resulting from the research program.

1.2.2 Workshop Participation

Subsequent to the research briefing, the Assessment Team participated in the Flight-Critical Digital Systems Technology Workshop held on December 13 - 15, 1988, at NASA Langley (hereafter referred to as the Workshop). [1] Four industry and one government speakers provided a perspective on the state-of-the-art in aerospace flight-critical systems. This perspective included discussion of industry trends as well as future requirements.

After these opening presentations, the workshop broke into seven working groups to assess the future needs of the industry. Each of the seven working group sessions was attended by members of the Assessment Team as shown in Table 1. Assessment Team members were assigned to these working groups according to their individual research experience and expertise. It was felt that knowledgeable observers would be in a better position to interpret and place into context the dynamic ebb and flow of discussions that are the essence of these dynamic group situations.

Subsection 2.2 of this report summarizes the working group needs as perceived by the Assessment Team members who attended the working group sessions. In addition to a summary of the working groups conclusions, the summaries may contain further comments representing the individual opinions of the Assessment Team members. This additional information is provided as further guidance to the assessment process.

1.2.3 Assessment Team Meeting

Immediately after the workshop an Assessment Team meeting was held to compare industry needs to the NASA Langley research program. During this meeting a consensus on industry needs gleaned during the workshop

[1] A separate report on the workshop entitled "NASA-LaRC Flight-Critical Digital Systems Technology Workshop" [1] is available.

Table 1: Assessment Team Coverage of Working Groups

Aeronautical Requirements	John E. Reed
Space Requirements	Janet R. Dunham
System Design For Validation	Anthony S. Wojcik Greg Chisolm Peter J. Saraceni
Failure Modes	Daniel P. Siewiorek
System Modeling	Eliezer Gai
Reliable Software	Janet R. Dunham
Flight Test	Cary R. Spitzer

was obtained and an assessment matrix of "Industry Needs vs. Research Programs" was derived.

1.3 Organization of this Report

The report is organized into four sections: an Introduction and Overview section on the Assessment Team and its review process; discussion on industry trends as perceived by the speakers on the first day of the Flight-Critical Digital Systems Technology Workshop, and a summary of each working group meeting of the workshop; a correlation of the Langley Research Center programs to the perceived industry needs; and finally, Recommendations.

The five appendices include the Assessment Team briefing agenda, the Workshop agenda, the Assessment Team members, comments on some of the activities under the NASA Langley Flight-Critical Research Program by a few Assessment Team members, and Assessment Team report summary viewgraphs.

2 Workshop Observations: Industry Needs

2.1 Industry Trends

Several trends were perceived from the guest speakers during the first day of the Workshop. The first is that the complexity of individual systems, such as flight control, were increasing. Second, more of the functions are being performed digitally as opposed to the more historic analog and mechanical technologies. Third, for economic reasons, more systems such as propulsion, air data, avionics, etc., were being integrated with flight control. This integration causes the "core" of flight-critical systems that require verification to increase by over an order of magnitude. Even though the individual subsystems may not be flight-critical, the fact that they are integrated with flight-critical subsystems requires verification that they will not interact in a harmful manner. Fourth, avionics is an ever-increasing item in terms of time and manufacturing costs of aircraft, approaching 50% of the cost in contemporary military aircraft.

Several issues were also perceived in system design. As system increases, the design effort increases in a nonlinear fashion due to the growing size of design teams. In particular, the communications overhead increases as the square of the number of people who need to communicate. Furthermore, if these communications are carried on in an individual fashion there is increased probability of inconsistency. These design teams are composed of multiple disciplines where each discipline contributes to the design concurrently rather than in a sequential fashion. There is early emphasis on dependability (e.g., reliability, availability, maintainability, safety) with computer-aided design tools for support. The concept of system-wide integrity management is emerging. Traditionally, problems have surfaced at the interface between disciplines where the communications is incomplete or ambiguous. The crossing of the subsystem boundaries means that assumptions need to be tracked to ensure consistency among the subsystems as well as identifying those subsystems effected by a modification or an update in another subsystem.

The technology to integrate and verify systems depends on the "ground rules" of the local situation. For example, a completely new system may have the freedom to develop a new approach, whereas an upgrade to an existing system probably requires an increment on the verification process originally used for the system. How can these incremental changes be verified? Often, details of the original integration and verification process have been lost. How can this information be preserved and used in future updates of the system as well as being transferred to new systems design?

There is also an increasing gap between the theoretical capabilities of the concept, as predicted by modeling or simulation, and that actually demonstrated in the field. How can this gap be diminished in general; in particular, how can the performance of new concepts be predicted without costly field evaluation?

At the same time as system complexity increases, the threats or "failure modes" to systems is increasing. Threats include intra/inter-system electromagnetic interference (e.g., there are a wider variety of sources for interference both internal and external to the aircraft), lightning, static discharges, high altitude electro-magnetic pulses, sabotage, and design errors. These increasing threats pose a significant challenge to both system design and verification.

The guest speakers offered many suggestions that could assist in the response to the above challenges.

- A methodology to develop and verify "requirements".
- A metric for predicting and evaluating complexity.
- A list of "safe" design features and their importance (e.g., Byzantine resilience, design diversity, etc.).
- Validation for nondeterministic systems, such as artificial intelligence/ knowledge-based designs.
- Validation of the support tools, such as computer-aided design and computer-aided manufacturing.
- Evaluation of new technologies and their impact on avionics systems, such as composite materials for air frames.
- Identifying other new technologies (e.g., fiber optics) to withstand lightning threats and Ada.

2.2 Assessment Team Working Group Reports

2.2.1 Summary of the Requirements for Flight-Critical Digital Systems — Aeronautical Working Group

John Reed
Federal Aviation Administration Technical Center

To put this assessment in the proper perspective, one must review the "sessions" definition of flight-critical digital system as provided[2]. Out of that discussion came the eight general discussion topics. From that came a listing of 21 research/needs and a set of six research requirements. After an extensive time of deliberations, a comprehensive set of ten recommendations for NASA/industry aeronautics research initiatives were developed. An assessment of the priorities and near term research initiatives is provided in this report.

First, if one is looking to implement competitive advanced flight control systems technology by the year 2000, the effort primarily is "near-term and high priority!" But, the research needs and recommendations defined by the aeronautical requirements working group will be taken as a point of departure for my assessment and priorities that are given in Appendix D.

The high priority needs are:

1. To acquire Electro-Magnetic Environment (EME), i.e., lightning, High Energy Radio Frequency (HERF), aircraft electrical hazards, static discharge, etc., data, threat definition analyses, modeling, upset studies, protection concept design, test and evaluation, etc.

2. Compilation and analysis of in-service experience, reliability, failure data, etc., for flight-critical systems, equipment, and components (i.e., down to solid state device level) must be acquired, understood, and sanitized.

3. Early on, as a part of the FAA Certification Process, the new technology certification basis must be developed for the FAA and industry air-

[2] See pages 13-14 of "NASA-LaRC Flight-Critical Digital Systems Technology Workshop"

craft/systems design, testing, and certification. Regulations, advisory material, guidelines, etc., must not inhibit technology implementation.

4. Cost and performance trade-offs must be accomplished for complex fault-tolerant systems (in light of the FAA's understanding and the certification process).

5. Cost and time effective verification and validation philosophies must be developed for "complex integrated systems."

6. Advanced analyses tools, i.e., modeling, fault insertion/tolerance, fault detection coverage, etc.

7. Structured requirements methodology tools need further development.

8. Structured design methodology tools need further development, i.e., automatic code generation, logic synthesis, etc.

9. System(s) stress testing (i.e., random failures, upset, inputs, noise, environment, etc.) must be pursued.

10. Advanced maintenance concepts over life cycle of aircraft, i.e., EME protection, safety, systems requirements.

Issues and concerns related to these needs are:

- Current FAA rules, regulations, Advisory Circulars, etc., inhibit advanced digital flight control and avionic systems innovation design, development, and implementation.

- FAA rules and regulations, if interpreted by Special Conditions, should be coordinated and developed with airlines, airframe, and systems designers prior to initiating a modification or new development, and not after the fact during the type certification process (get user, manufacturer, and FAA together right up front).

2.2.2 Summary of the Requirements for Flight-Critical Digital Systems — Space Working Group

Janet R. Dunham
Research Triangle Institute

The space requirements working group addressed issues of changing requirements in space applications (e.g., the aerospace plane, the shuttle, the launch vehicles, earth orbiting satellites, the space station, and planetary craft). Discussion focused on the joint Air Force/NASA Advanced Launch System as an example of current requirements.

In the past, high reliability was achieved by using extensively tested single string systems with redundancy being employed for crucial single point failures. This approach resulted primarily from restrictions on system weight and power consumption. The working group established a consensus that technology advances in hardware, software and fault-tolerant system architecture; the increase in lift capability; and more demanding application requirements dictate the need to reassess space vehicle requirements for fault-tolerant avionics.

Critical issues addressed during the working group included what were appropriate figures-of-merit for avionics use in space applications, systems costs and testing, system engineering and integration, and requirements for future systems.

Key working group recommendations included addressing what the appropriate figure of merit for system design is (e.g., cost, reliability, time coverage, and availability), defining an approach to specifying parts levels (i.e., Class S vs Class B), and an increased emphasis on integration research activities such as integration of a health monitoring interface and validation of adaptive GN&C/intelligent systems.

2.2.3 Summary of the System Design for Validation Working Group

Anthony S. Wojcik,
Michigan State University/Argonne National Laboratory
with the assistance of
Greg Chisholm, Argonne National Laboratory
and
Peter J. Saraceni, Federal Aviation Administration Technical Center

The stated focus of this Working Group was the question of how can flight-critical digital system technology be made part of initial vehicle design and thus escape the traditional "add on" role of electronic systems? The group initially reviewed the issues of verification and validation and addressed the scope of the design for validation problem.

Validation was defined to be the process by which it is determined that the specifications of the system as a whole are correct and meet the overall system requirements. Verification was defined to be the process whereby it is determined that the hardware and software implementation of the system meets the specifications.

It was noted that the complexity of individual avionics systems was increasing and that there was a trend toward the integration of various digital-based systems. The result is that the "core" of what will have to be verified will expand by an order of magnitude. The consensus view was that verification was hard enough and that validation is even more difficult. Further, it is impossible to get control of the overall complexity of a flight-critical system with current techniques and tools for design and analysis. It became apparent that what was needed was an overall methodology of system engineering. The methodology needed to incorporate the principles of modularity, and it was indicated that a mathematical basis for design and formal analysis was greatly desired.

The Working Group spent a considerable amount of time discussing the features of a design methodology and the development of an integrated tool set for system engineering. Fundamentally, the methodology is to be based on a "common language" that could be used from "requirements specification" to "rollout". Hence, a hierarchical design methodology is needed.

There was a desire to have a "language" that would support a common database. The database would be accessible via the "language" to all the actual "tools" that would be developed. It was noted that the accepted view of the "language" was that it should serve as a means to help the designer to keep track of information (a bookkeeper) and that the "language" was not yet to be viewed as a "design assistant."

The Working Group generated a long list of features that were desirable of the methodology. Discussion indicated that many of these features would require further research for appropriate "tools" to be developed and integrated into the methodology. The following list contains most of the major "tools" that were desired. It should be noted that the Group wanted "tools" that would be capable of analyzing each of the concepts contained in this list with the expectation that the "tool" would either provide information about the usefulness of the concept for a specific phase of the overall design or provide useful analysis of the concept for a specific design phase.

1. Applicability of n-version software and hardware.

2. Tradeoffs between performance and fault tolerance.

3. Partitioning of functions between hardware and software.

4. Applicability of concurrent (parallel) processing for performance enhancement.

5. Complexity metrics and approaches to complexity reduction.

6. Impact of the operational environment.

7. Testability.

8. Performance evaluation and simulation.

9. Verification techniques.

From this list, one can see that there was a strongly expressed desire to have an integrated approach to the design process.

It was evident from the discussion that there was hesitancy on the part of some to move toward the development of such a methodology. Fundamentally, the hesitancy was based on the unwillingness to invest in such a procedure and to commit to use a standard system that would be shared by all the constituents of the industry. Further, there was the question of how to compel the industry to make use of such a common methodology. The point was made that international competitors either have or will be developing such a methodology. If the aerospace industry does not face the challenge now, it faces the same problems that the automobile and semiconductor industries have faced.

Also apparent was the fact that there is a recognition that digital- based systems were needed, but that there was also concern about such systems. Some even suggested the need for mechanical back-ups. The importance of the integrated design of hardware and software was recognized, but not fully appreciated. The lessons of the computer industry in which hardware was in some cases developed virtually independent of software considerations have not been learned. It could also be seen that while "parallel computing" was a concept that could help, there was broad disagreement about what "parallelism" meant.

It became clear that the role for NASA was to take the initiative in the development of the methodology for system engineering. NASA could work on the "language" and "database" issues and work with the industry to accept them. NASA could show how the "database" can be developed, how it can be used, and how "tools" can be designed to interact with the "language" and "database". It would be essential to obtain a commitment from industry to use the NASA developments as well as a commitment from NASA for the long-range support of these items.

2.2.4 Summary of the Failure Modes Working Group

Daniel P. Siewiorek
Carnegie-Mellon University

The charter of the Failure Modes working group was to determine how the various failure modes impact the design of flight-critical digital systems. Three recommendations were presented to the Workshop as a whole that were deemed to have high priority.

1. EME/HERF research. Design verification criteria should be developed for these threats. The analysis capability should include models of the transfer process of coupling of the energy from the external environment to the internal units including boxes and connectors. The system and vehicle responses should be predicted as a prelude to verification

testing. Accelerated life testing on new technologies such as fiber optics designed to combat these threats should also be conducted.

2. Testing. Research is required to improve troubleshooting and diagnostic aids so that troubleshooting and line-replaceable unit turn-around times are diminished. Quantification and verification of the effectiveness of various techniques should be studied including error detection/correction approaches. Guidelines should also be developed for injecting faults which assess the performance and capabilities of these detection and correction techniques.

3. Component trends. An on-going test program which provides empirical data on new families of digital devices should be developed. The data should include: energy thresholds for upset, failure modes, and annual updates to Mil Handbook 217.

Two long-term goals were identified:

1. Effectiveness and optimization of redundancy techniques including cost versus risk analysis criteria. The best methods for tolerating threats should be catalogued along with their effectiveness and guidelines for incorporating them into the design process.

2. Data collection from 1975 to the present of single point failures and domino events leading to vehicle loss.

This Assessment Team observer noted that the working group focused on the EME/HERF threats. This observer believes the above recommendations should be expanded to include other threats such as static discharges, high altitude electro-magnetic pulses, sabotage, and design errors. Sabotage in forms such as computer viruses should not be ignored. Future aircraft will be composed of a network of computers which will be periodically connected to other computer facilities such as maintenance. These other facilities will in turn be connected to yet other networks and eventually some computer node will be connected to a regional or national network. We should not underestimate the ability of innocent or purposeful propagation of software-altering programs.

2.2.5 Summary of the System Modeling Working Group

Eliezer Gai
The Charles Stark Draper Laboratory, Inc.

I attended the system modeling working group that was chaired by Phil Babcock and had about 12 participants. I did not take part in the discussions (except for a short while in the beginning) and this summary reflects my own impressions of the discussions blended with impressions from individual talks that I had with several members of the group (including all the Draper participants), and influenced strongly by my own unbiased opinions.

The discussions, centered (too heavily) on the tools that are currently available for reliability evaluation. Even though there was some disagreement as to which tools (or underlying theories) are the best, it was clear that industry needs are mainly in understanding of how to use the available tools efficiently and how to gain confidence in the results that are obtained using those tools. The implication was that the theoretical basis for reliability evaluation is well-founded (NASA Langley efforts have contributed enormously to that cause) and the focus in the future should be on improving users interface. I feel that the efforts to improve the interface should not be done by NASA since they do not constitute new research, but rather be developed on a commercial basis.

The open research areas are in expanding the tools' capabilities to include performance, performability, and life cycle effects. The Advanced Launch System (ALS) is a case in point. The requirements are not for reliability only, but also for the probability of payload insertion within a given error footprint in position and velocity. In addition, the tight requirements for cost per pound require a cost analysis that will include the effects of losing the payload as well as missing the footprint. Some work has been done in this area, particularly for space vehicles. More research can be done in this direction for aircraft flight-critical systems where performance requirements are not uniquely defined. It seems to me that this is a good area for NASA to perform follow-on research.

I feel that there is some confusion within industry with regard to the notion of what tools can do. Tools will never replace capability, and the real issue for the industry is either to develop a capability inhouse to deal with system modeling, or to contract somebody to do it for them. The capability issue is the same as in design of control systems and the fact that there are now good control design tools did not change the issue. In contrast to what I heard in the discussions, industry needs people with systems analysis background rather than people with knowledge of stochastic processes in order to develop this capability. Using the control analogy again, to design a control system you need knowledge of dynamic systems theory and not knowledge of measure theory. In addition, similar to the argument that it is not important whether you use classical or modern control theory as long as you do it right, it does not matter whether you use Markov or combinatorial analysis in system modeling.

How one goes about building this capability is another important issue. It is hard to draw people to the field for two reasons. Reliability modeling does not have a good image, and there are very few schools that have classes available on this subject. I think that NASA can contribute in this area by organizing workshops that will include a short course on the subject, work on a common problem, and have discussions on specific problems that industry has with their programs.

2.2.6 Summary of the Reliable Software Working Group

Janet R. Dunham
Research Triangle Institute

Concern over the problems associated with developing and validating the reliability and safety of software used in flight-critical systems has increased since the 1981 NASA Langley sponsored meeting that addressed these issues. The reliable software working group re-addressed many of these issues and added a few new ones (e.g., validation of software development tools and expert systems, and the role of Ada) with discussion focusing on how software should be treated as a component of flight-critical systems.

The reliable software working group discussion was broad and an emphasis was placed on involving all the working group participants. It yielded a consensus on the major software issues as well as a comprehensive, detailed, and prioritized list of research activities.

The following unprioritized list reflects my independent assessment of the major points made.

- Technology Development in support of additional standards and guidelines for development of real-time avionics software is needed.

- Cost/benefit analysis of Fault-Tolerant Software Strategies focused on:

  1. comparison for fixed cost with other verification, validation, and test strategies
  2. development and evaluation of various voting strategies
  3. data collection and analysis for real-world systems; in particular, degree of independence, configuration management, and cost issues

- Development and evaluation of single version software. Specific issues include:

  1. evaluation of effectiveness and determination of ways to improve various test strategies (e.g., automated and semi-automated generation of test cases, test effort planning, new strategies)
  2. effectiveness of software safety techniques (e.g., software fault tree analysis, software failure modes and effect analysis, and software hazard analysis)
  3. contribution of proof of correctness techniques for establishing software integrity
  4. data collection and analysis of real-world systems
  5. effect of Ada on achieving reliable flight-critical systems

- Definition of Requirements for Verification, Validation and Test (V,V&T) of Software Development Tools

- Development of tools for maintaining, enhancing, and retargeting flight-critical software

- Development of Tools and Criteria for V,V&T of AI systems (e.g., expert fuel handling, emergency management)

- Software Modeling and Measurement

1. evaluation and refinement of product and process measures vs. achieved reliability and safety
2. address difficulty in quantitatively measuring and modeling software reliability when ultra-reliability requirements are being levied (e.g., complementary validation of models, breakthroughs in statistical theory that are necessary)

- Systems Issues
    1. evaluate partitioning strategies (e.g., techniques for establishing software error containment regions and criticality partitioning)
    2. Software implemented fault tolerance for diagnostics/maintenance
    3. measurement and descriptive characterization of hardware and software errors for on-line detection and diagnosis

These key points were reflected in the construction of the reliable software portion of the matrix provided in Section 4.

Based on my involvement in software research and development projects sponsored by both government and industry, I recommend that NASA Langley begin to incorporate software research results into a tailorable software reliability evaluation environment. This environment could contain:

1. verification and validation (v&v) tools (e.g., test, safety analysis, CASE related analysis, and formal verification tools)
2. software metrics and reliability growth models with calibration/refinement from operational usage
3. software reliability engineer's assistant functions. For example,
    (a) knowledge base of error data for feedback to developers (e.g., causal analysis for future defect prevention)
    (b) a knowledge base of modeling and analysis procedures

Components of this environment could then be used by industry and in future research projects. As more effective tools and techniques are developed and more research data is acquired they could be integrated into this environment.

2.2.7 Summary of the Flight Test Working Group

Cary R. Spitzer
NASA Langley Research Center

Flight testing of digital systems is where the electrons meet the tarmac.

The recommendation of the Flight Test Working Group is "NASA flight-critical systems research program should develop and demonstrate this process ('systematic design, test, evaluation and validation') including flight test."

Flight testing is mandatory to demonstrate that systems developed using current assessment and validation models and tools will work. It validates these models and tools and, to a lesser extent, the system. (Because of the large number of possible states in a digital flight control system, complete validation of a system in any reasonable flight test program is impossible.)

The Flight Test Working Group feels that flight testing is an integral part of an iterative, closed-loop process whereby experience gained in building, laboratory evaluation, and flight testing of a real, flight-critical system is fed back into modifications and enhancements of the system and, more importantly from the workshop viewpoint, into the refinement of the assessment and validation tools.

Focusing on real flight hardware brings out system integrity and system functionality issues. Typical system integrity issues include hardware/software compatibility; fault detection, isolation and recovery; timing; and hardware interfaces with sensors, actuators, and other aircraft systems. Typical system functionality issues include pilot/vehicle interface; envelope limiting; and automatic flight control, e.g., flutter suppression, autonomous landing and autonomous windshear guidance.

The Flight Test Working Group recommends the construction and flight testing of a vehicle management system that embodies the important system integrity and functionality issues. The system should include:

- Fly-by-wire or fly-by-light flight controls
- Crew station displays
- Autonomous landing
- Windshear prediction
- Flutter suppression

3 Industry Needs vs. Research Programs

The Assessment Team compared the industry needs defined during the Flight-Critical Digital Systems Workshop to the NASA Langley flight-critical systems research program. This comparison was conducted immediately after the workshop during a single afternoon meeting. The objectives of this comparison were:

- to obtain a consensus on the industry needs gleaned during the workshop, and
- to assess the coverage of the industry needs by the NASA Langley in-house flight-critical systems research program.

Both these objectives were accomplished by the Assessment Team, the results of which are summarized below.

3.1 Consensus Viewpoint on Industry Needs

Each Assessment Team member provided their viewpoint on the industry needs identified during the workshop. These viewpoints were then combined into a single list and categorized by a general research topic that would address these needs. The general topics identified were validation, assessment, design, EM upset, data collection, and maintenance. Table 2 defines this list.

Once the combined list of needs was created, each team member present cast four votes reflecting what they considered as the highest priority needs. The results of this voting are shown in Table 3 . Industry needs with equal number of votes were assigned the same priority. Industry needs receiving zero votes have been omitted from this Table. Members of the Assessment Team (who were present during the vote) unanimously agreed that a validated hierarchical integrated tool set was the most important industry need.

3.2 Current Research Program Coverage of Industry Needs

After reaching this consensus, the Assessment Team proceeded by mapping the industry needs to the NASA Langley in-house research program. This mapping is shown in the matrix given in Table 4 . The rows of this matrix correspond to on-going in-house NASA Langley flight-critical research programs that were reviewed by the Assessment Team. The columns correspond to industry needs organized by the general research topics previously established in Table 2 . The matrix cells depict the numbers corresponding to the industry needs listed in Table 2 . Some of these tasks have the letter **F** or **P** or a ? associated with them where these letters describe the current coverage of the research activities:

F Full coverage; i.e., Aware of all approaches proposed during workshop

P Partial coverage; i.e., Only working on part of the problems identified by the workshop

? Insufficient information for determining coverage

The matrix cells below the solid double line contain recommended areas for new research tasks. The matrix applies to methodologies for V & V through the total life cycle, including the cost- and time-effectiveness of the methodology for complex integrated systems.

This mapping activity resulted in the following observations with respect to the coverage of the current research program:

- all tasks under the current research program are at least partially addressing the industry needs listed in Table 2 .
- except for Industry Need 5.1, In-service Experience, the research program is addressing (with varying degrees of coverage) the higher priority industry needs identified in Table 3 .
- due to funding limitations there are a significant number of industry needs either not being covered or not being covered adequately.
- the current program is front-end loaded in terms of the life cycle.

From these observations, the Assessment Team concluded that the research program was on track in meeting industry needs and could benefit from additional dollars to provide more coverage of these needs.

Table 2: Industry Needs

Research Topic	Industry Need
Validation	1.1 System Stress Testing (Test for random failures, upset, inputs, noise, environment, etc.)
	1.2 Validated Hierarchical Integrated Tool Set (Address overall validation issues through the integration of mathematically-based design and analysis tools.)
Assessment	2.1 Modeling Tools (Develop and verify individual easy-to-use modeling tools that address reliability, performance, coverage and cost.) 2.2 New Algorithms (Address difficulties in measurement and modeling of hardware and software reliability when ultra-reliability requirements are being levied.)
	2.3 System Design Figures of Merit (Determine appropriate set)
Design (hardware and software)	3.1 Cost Trade-off and Effectiveness of Design Methodologies and Fault Tolerance Concepts (Conduct studies to compare effectiveness for fixed cost among techniques, evaluation of voting strategies, and data collection and analysis of real-world systems.)
	3.2 Verifiable Building Blocks (Address issues related to modular construction and reusing components of verified reliability.)
	3.3 Formal Verification (Improve tools and methods and evaluate design proof effectiveness.)
	3.4 Life Cycle Considerations During Design (Address performance, reliability, testability, and cost.)
EM Upset	4.1 Threat Modeling, Propagation Analysis and Testing (Develop design verification criteria for threats, in particular EME/HERF related.)
Data Collection	5.1 In-service Experience (Compile and analyze in-service data and develop monitoring systems.)
Maintenance	6.1 Modeling, Design for Maintenance after Certification (Develop tools for maintaining, enhancing, and retargeting flight-critical software.)

Table 3: Higher Priority Industry Needs

Priority	Industry Need	Research Topic	Number of Votes
1	1.2 Validated hierarchical integrated tool set	Validation	6
2	3.1 Cost trade-off and effectiveness of design methodologies and FT concepts	Design (h/s)	5
3	2.1 Modeling - ease of use, verification, cost/performance	Assessment	4
3	4.1 Threat modeling, propagation analysis & testing	EM Upset	4
4	5.1 In-service experience	Data Collection	3
5	2.2 New algorithms	Assessment	1
5	3.2 Verifiable building blocks	Design (h/s)	1

Table 4: NASA Flight-Critical Systems Research vs. Industry Needs

On-going/In-house	Industry Needs						
IN-HOUSE RESEARCH PROGRAMS	VALIDATION	ASSESS-MENT	DATA/ DESIGN	EM	COLLEC-TION	MAINTE-NANCE	COMMENTS
<u>Validation</u>							
Mathematical Verification			3.3F				
Knowledge-Based Systems		2.2?					
Advanced Information Processing System (AIPS)	1.1P		3.2P				Other generic sets possible
Integrated Airframe Propulsion System Architecture (IAPSA)			3.1P				One application with one building block set and reliability and performance being the only measures used
<u>Assessment</u>							
Reliability Analysis Tools		2.1P					Missing other metrics such as cost/performance
Fault Simulation		2.1F					Full coverage for threats addressed
<u>SW Reliability & FT</u>							
Software Reliability			3.1P				Effectiveness of safety and test techniques
FT S/W			3.1P				Data collections of real FT systems
<u>EM Upset</u>							
Upset Research at Langley				4.1P			Other threats
Recommended Areas for New Research Tasks	1.1 1.2	2.1 2.2 2.3	3.1 3.2 3.4	4.1	5.1	6.1	

4 Recommendations

4.1 General

Within the scope of the activities conducted, the Assessment Team has found the research program to be very sound. All tasks under the current research program are at least partially addressing the higher priority industry needs. However, the workshop generated many more critical research needs than the Information Systems Division has resources. The team recommends that the program resources be substantially expanded to give adequate coverage to the existing research and extended to additional areas identified in Table 2 .

4.2 Specific

1. The current program is front-end loaded in terms of the life cycle and needs to be extended into downstream activities to include operations and maintenance.

2. We recommend initiation of research tasks in the following areas:

    (a) the development of a validated hierarchical integrated tool set that can be used to address issues related to life-cycle validation

    (b) the conduct of cost-tradeoff and effectiveness studies of design methodologies and fault tolerance concepts

    (c) the development and verification of easy-to-use modeling tools that address reliability, performance, coverage, and cost

    (d) the conduct of threat modeling, and propagation analysis and testing. In particular, develop design verification criteria for Electromagnetic Environment(EME)and High Energy Radio Frequency (HERF) related threats.

    (e) the compilation and analysis of in-service data

3. In order to focus the research program, we recommend the selection of an actual hardware and software system that is under development as a vehicle for an ongoing evaluation of the emerging technology.

4. We recommend that personnel attend more applications-oriented conferences (e.g., AIAA, IEEE, SAE) in addition to research conferences.

5. We know there are other advisory committees and a peer review process; however, we suggest that a standing industry/academic oversight committee be established. The committee should meet annually to review the internal/external research sponsored by the branch. The purpose of this committee is to help focus the research and effect technology transfer. The long term nature of this committee would provide continuity in tracking progress, thus yielding an historical perspective of the benefits of the research program in lieu of a single snapshot.

6. To assist in technology transfer:

   - We propose that the AIRLAB Interface be published on an annual basis and expanded to include all supported research projects. The circulation list should be expanded.
   - We suggest that workshops combining the modeling tool builders and users be held.

References

[1] C. W. Meissner, J. R. Dunham, and G. Crim, Eds. NASA-LaRC Flight-Critical Digital Systems Technology Workshop. NASA Conference Publication 10028, April 1989. Contract NAS1-17964 Task 29.

APPENDIX A

ASSESSMENT TEAM BRIEFING AGENDA

ASSESSMENT TEAM BRIEFING AGENDA

December 6, 1988, Building 1220, Room 110

8:30 a.m.	Welcome	Creedon
8:45 a.m.	Introduction	Meissner
9:15 a.m.	AIPS	Pitts
9:45 a.m.	IAPSA	Palumbo
10:15 a.m.	Fault-Tolerant Software	Eckhardt
10:45 a.m.	Software Reliability	Finelli
11:15 a.m.	Redundant VHSIC	Hayes
11:45 a.m.	Lunch	
1:00 p.m.	Mathematical Verification	Butler
1:45 p.m.	Reliability Modeling by Path Analysis	Butler
2:15 p.m.	System Upset	Belcastro
2:45 p.m.	Reliability Modeling by Behavioral Decomposition	Bavuso
3:30 p.m.	Fault Simulation, G-GLOSS	Bavuso
4:00 p.m.	Assessment Team Meeting	

APPENDIX B

WORKSHOP AGENDA

Flight-Critical Digital Systems Technology Workshop

Agenda

December 13, 1988

9:00 a.m. — 12:00 noon: Opening Session (Overview Talks)

9:00	Dr. J.F. Creedon, NASA Langley Research Center
9:30	Dr. Thomas B. Cunningham, Honeywell Systems Research Center
10:00	Dr. Carl S. Droste, General Dynamics
10:30	Mr. Jim Treacy, Federal Aviation Administration
11:00	Mr. Larry J. Yount and Mr. Richard F. Hess Honeywell Commercial Flight Systems
11:30	Mr. Richard S. Ullman, ITT Defense Technology Corporation

1:00 p.m. — 5:00 p.m.: First Parallel Working Groups Session

- Requirements for Flight-Critical Digital Systems — Aeronautical
- Requirements for Flight-Critical Digital Systems — Space
- System Design for Validation
- Failure Modes
- System Modeling
- Reliable Software
- Flight Test

December 14, 1988

8:30 a.m. — 12:00 noon: Second Parallel Working Group Session

1:00 p.m. — 5:00 p.m.: Third Parallel Working Group Session

December 15, 1988

8:30 a.m.	Chairmen's Reports
12:30 p.m.	Workshop Adjourns

APPENDIX C

ASSESSMENT TEAM MEMBERS

ASSESSMENT TEAM MEMBERS

Professor Daniel P. Siewiorek, Chairman
Dept. of Computer Science and
Electrical/Computer Eng.
Carnegie-Mellon University
Pittsburgh, PA 15213
(412) 268-2570
dps@a.gp.cs.cmu.edu

Mr. Cary R. Spitzer, NASA Representative
NASA Langley Research Center
Mail Stop 265
Hampton, VA 23665-5225
(804) 864-3854

Ms. Janet R. Dunham, Coordinator
Center for Digital Systems Research
Research Triangle Institute
P. O. Box 12194
Research Triangle Park, NC 27709
(919) 541-6562
jrd@rti.rti.org

Mr. Greg Chisholm
Argonne National Laboratory
9700 S. Cass Avenue
Argonne, IL 60439
(312) 972-6815
chisholm@mcs.anl.gov

Dr. Eliezer G. Gai
The Charles Stark Draper Lab., Inc.
MS 4B
555 Technology Square
Cambridge, MA 02139
(617) 258-2232

Mr. John E. Reed
FAA Technical Center
ACT-340
Atlantic City Airport, NJ 08405
(Pete Saraceni 609-484-5577,
review substitute)
(609) 484-4135

Mr. Herman Schmid
General Electric Company
P. O. Box 5000
Binghampton, NY 13902
(607) 770-2764

Dr. Anthony S. Wojcik
Professor and Chairman
Computer Science Dept.
Michigan State University
East Lansing, MI 48824
(517) 353-6484
wojcik@cps.msu.edu

APPENDIX D

COMMENTS ON SELECTED ASPECTS OF THE NASA LANGLEY FLIGHT-CRITICAL RESEARCH PROGRAM

COMMENTS ON
SELECTED ASPECTS OF
THE NASA LANGLEY FLIGHT-CRITICAL
RESEARCH PROGRAM

This appendix provides summaries of material that partially supported the Assessment Team in making the recommendations contained in this report. These summaries were prepared by four different team members and do not implicitly reflect the consensus viewpoint of the entire team.

NASA LANGLEY FLIGHT-CRITICAL RESEARCH PROGRAM

Evaluation of Industry Relevance at NASA Langley

Daniel P. Siewiorek
Carnegie-Mellon University

For over two decades NASA Langley has been a leader in high-dependability airborne computer systems. During the 1970's, the pioneering work in the Software Implemented Fault Tolerance (SIFT) and Fault Tolerant Multiprocessor (FTMP) architectures had far-reaching impact on the architectures of aerospace computer systems.

Throughout that period and continuing, NASA Langley has made effective use of external panels from academia and industry to not only assess but also to help formulate research programs. These panels are often constituted by the internationally recognized leaders in reliable and fault-tolerant systems.

The typical flight-critical systems research program is composed of between one and four in-house or on-site personnel with an annual discretionary budget of $100,000 to $500,000 for external purchases such as equipment and university/industry contracts. Since typically three full-time personnel are required to form critical mass in a research area, the current FCS staff seems to be spread thinly among the various research programs. Resources are insufficient to carry out the research agenda. This is the classical dilemma of a research program manager - whether to support fewer projects which all attain critical mass or to support a broader range program so that the various interrelated technologies are tracked. Whereas the "pinnacles of excellence" approach provides deep penetration and substantial results in a narrow area, the broad based approach might be more appropriate for a government agency which is responsible for a wide area. The current NASA Langley approach with technically-active, in-house researchers covering a broad range of topics with selected external contracts providing penetration and depth appears to be the appropriate model for the FCS. The external contracts can be expanded or reduced as a function of available funding without impacting the stability of the in-house organization. At this point in time, especially with respect to the modeling tools, transfer of technology to industry is critical to reap the benefits from the research program. The current approach to technology transfer is not completely effective. Furthermore, a more effective program will require additional resources from industry/government.

The NASA Langley work on software reliability and fault tolerance is one of the few government-funded programs which is attempting to place the art of reliable software on a firm scientific and application basis. The conception, careful construction, execution, and data analysis of software experiments is essential for understanding the fundamental creative process of systems design. The cross-fertilization and reuse of experimental data between the software reliability and fault-tolerant software programs is not only imaginative but also provides several independent interpretations of the experiments. The data from these experiments provides concrete evidence to settle differences between basic design approaches which heretofore have been justified on the basis of intuition. Similar experiments for evaluating the effectiveness of other software verification and validation techniques such as safety analysis and software testing should also be addressed.

Verification and validation is essential for complex computer systems which control flight-critical functions. The Information Systems Division is pursuing several approaches to verification and validation. The mathematical modeling and supporting software packages (e.g., CARE III, HARP, SURE) developed through the last two decades represent the most advanced, cohesive program in this area. The program has been particularly effective since each succeeding generation of models built on the experience of the previous generation. The software packages and models developed by the System Validation Method Branch have had a strong influence upon selected academic and industrial projects although they have not been universally adopted. As the limitations of modeling as a verification approach have become apparent, other approaches such as fault injection/simulation, formal proofs and hot bench are being explored. Other approaches such as iron bird and flight test have yet to be used. In the realm of simulation, several commercial packages have become available which may be sufficient to perform the requisite functions. For example, Gateway Design Automation has a simulator, VERILOG, which supports descriptions all the way from the gate level through the register transfer and behavioral levels on up to statistical architectural simulation. A companion simulator, VERIFAULT, does fault simulation and has already been deployed in parallel versions. These commercial tools should be explored to see if they can fulfill the FCS and industrial missions.

The area of mathematical verification remains controversial as to its effectiveness on real problems. However, there is a group of researchers advocating that the current limits of mathematical verification should become constraints upon the fundamental design methodology. For example, in a network rather than produce a different protocol for each of the hierarchical levels it may be superior to define a single mechanism which, when recursively applied, can produce protocols at all of the various levels. Not only would this single mechanism be better understood by the designer and perhaps lead to some economies in the design process, it would also represent a single building block to mathematically verify. This, however, is a very long term approach in that it requires not only a proof of concept but also a fundamental change in how systems are designed. While this is a massive undertaking, it should not detour effort from initiating a research program. In order to focus attention, we recommend the selection of a real subsystem that is under development as a vehicle for an ongoing evaluation of the emerging technology.

The fault-tolerant Very High Speed Integrated Circuit (VHSIC) effort suggests a mechanism for not only reaching critical mass but also for testing concepts such as an entirely new design methodology. Whereas the fault-tolerant VHSIC project is constrained to use industrially-supplied modules, the available manpower and the research leadership is insufficient to build a true fault-tolerant system. Yet there is expertise within the branch in modeling, software reliability, replicated system failure modes and solutions, and mathematical verification that could be brought to bear for a total system solution. The branch may wish to consider the augmented approach to research which periodically (with the period specified by the confluence of a set of maturing technologies - but perhaps no more frequently than once a decade) embark upon a system specification, design, construction, and validation[3]. This would not only transfer technology between the internal programs supported by the research, but it would also give those individual research programs a concrete, detailed example. This example would serve to illuminate holes in the current research results and help set future direc-

[3] The complexity of the target system could range from a simple, couple of man-year effort to a complex integrated system concept such as the ACEE-EET initiative.

tions for individual research projects. Likewise, the project could be a good demonstration vehicle for transferring technology to industry. It would be a testbed for such radical design methodology changes such as simplification for mathematical verification. Some of the low level work such as board layout and manufacturing could be contracted out to one of many commercial board fabrication services. The fault-tolerant VHSIC project in particular could have benefited from such an approach.

The issue of technology transfer to industry is a difficult one. As the Integrated Airframe Propulsion System Architecture (IAPSA) program indicated, NASA-sponsored external research is often required to gain the interest of industry. Subsequently, the industrial team goes through some of the same learning curves that NASA has already been through. Since these industrial teams are typically researchers with no deadline responsibilities for generating aerospace systems, the technology transfer more closely approximates osmosis than a direct infusion of technology. However, industrial participation is essential for producing realistic mission requirements and for providing timely feedback on the strengths and weaknesses of tools and methodologies in real design situations.

Another major form of technology transfer is reports. There is typically a long lead time between completion of the research and the availability of the reports. Furthermore, these final reports are often voluminous and difficult to read due to their detail. While workshops help transfer information at a point in time, they are still only one time events which only transfer information to those who were in attendance. Perhaps video tapes representing overviews of NASA projects and limited to 30 minutes in duration would provide a way of transferring technology that transcends the workshops. Furthermore, these video presentations could be transcribed into documents for leisure reading when VCR's are not available. The software tools that NASA produces is also another opportunity for technology transfer. Frequently these tools are stand-alone with only rudimentary man-machine interfaces. While the core computational engines represent the research contributions, the tools need to be integrated into existing CAD environments using input data from standard data bases and with easy to use and graphics-oriented human interfaces. The code for the computational engine perhaps represents less than a third of the code for a successful commercial product. It would be interesting to see if there could be a more formal mechanism for coupling the public domain computational engines produced by NASA into commercial CAD environments. It is only when the tools are available to the systems designer in a form that is convenient to use that the true impact of the research will be felt.

Personnel should attend both research and applications-oriented conferences (e.g., American Institute of Aeronautics and Astronautics (AIAA), Institute of Electrical and Electronics Engineers (IEEE), Society of Automotive Engineers (SAE)).

Data collected from actual ground-based commercial systems indicates that the sources of computer system outage are fairly evenly divided between hardware, software, maintenance, operator mistakes, and environment. The NASA Langley research program has focused on architectures to tolerate hard failures, design errors in hardware/software, and environment such as lightning strikes and single event upsets. The workshop identified several new areas of research including tolerance of other threats (i.e., HERF, sabotage, etc.), down stream concerns such as fault-tolerant man-machine interfaces for both operations and maintenance, etc. Research programs should be developed in these areas accompanied by appropriate levels of additional funding.

Some Comments On NASA Langley's Development Projects

Herman Schmid
GE, Binghamton, NY

AIPS: Advanced Integrated Processing System

With the integration of flight-critical systems, such as the Vehicle Management System (VMS) for the Advanced Tactical Fighter (ATF), there is a definite need for highly reliable multiprocessor systems.

The PAVE PILLAR and Advanced System Avionics (ASA) architecture developments funded by the Avionics Lab at Wright-Patterson Air Force Base are based on a distributed multiprocessor system in which processors are interconnected by a quad-redundant high speed (100 MHz) fiber optic token-passing data bus. Employing such an advanced concept in the next fighter aircraft causes great concern in flight control circles, since there are still no methodologies to verify and validate such an advanced system.

I believe that AIPS can overcome some of the major problems in verifying and validating multiprocessor configurations, since its key feature is the use of verified building blocks.

However, what I have not seen yet is a methodology that verifies any combination and configuration of verified building blocks, such as the Fault Tolerant Processor (FTP) in all required operating modes.

Is source congruency essential for verifying the FTP operation? Implementing this feature adds not only hardware and raises failure rates, but also increases cross channel data transfer and thereby introduces the potential for more transmission faults. The additional burden may be justified for a system requiring a mission reliability of 10^{-9}, but not for systems with a 10^{-7} requirement, especially when we have no idea what the magnitude of the probability of Byzantine faults is.

IAPSA: Integrated Airframe Propulsion System Architecture

While FTMP, SIFT, and AIPS consider only the digital processing portion of future control systems, IAPSA is the first one that addresses the Input/Output (I/O) functions, which in many applications are just as complex, or even more so, than the processing functions and just as challenging. To achieve this, IAPSA proposes to use a reconfigurable fault-tolerant network to interconnect up to 20 I/O nodes.

The hardware needed to implement this network, even if built with custom ICs, significantly impacts overall system size, weight and cost. However, even more disturbing is the complexity of the reconfiguration scheme, which is equal to that of a set of distributed multiprocessors. Consequently, it might be just as difficult to verify and validate such a network as it is for a reconfigurable multiprocessor system. A Boeing analysis showed also that the network offers little improvement in reliability over a quad-redundant I/O bus. Finally, the network assumes smart sensors and actuators, which still pose such key problems as: 1) operation in harsh environment, 2) cost of supplying redundant power to each node, and 3) maintenance access in hard-to-get-at locations.

However, although the results on this reconfigurable I/O network study are not very promising, the program is definitely attacking the right problem, because unless progress is made in the I/O field, the overall size, weight, cost and reliability of future control systems will be dictated by the I/O.

SURE: Semi-Markov Reliability Evaluation

Semi-Markov Unreliability Range Evaluator (SURE) is a very simple, elegant (slick) and cost effective system reliability estimation tool, especially when considering that it was practically developed on a "shoe string." The addition of Abstract Semi-Markov Specification Interface for the SURE Tool (ASSIST) now offers the much needed input capability. With it, SURE might even be called "user friendly."

But SURE also has it limitations, especially with respect to its ability to handle large systems. Hence, additional efforts should be made to overcome this limitation. I would like to see, for example, a study to determine if it would not be possible to give it the capability to handle large systems in a hierarchical multi-level fashion.

Airlines Need for Economic Analysis of Flight-Critical Systems

Cary R. Spitzer
NASA Langley Research Center

The airlines avionics community is developing requirements, such as higher reliability and a capability for periodic maintenance (vis-a-vis the current on-condition maintenance), for avionics systems on aircraft that will be entering service in the mid-to-late 1990s. The airlines believe that if these requirements are properly implemented, they will lead to reduced operating costs.

In response to these requirements, the airframers have proposed several distributed, highly-integrated, flight-critical avionics architectures, known as the Integrated Modular Avionics (IMA) concept. IMA will be similar to the Vehicle Management System of the Air Force PAVE PILLAR architecture.

The IMA architectures proposed by the airframers are based on advanced technologies such as fault-tolerant hardware and software, and extensive replication to permit user-transparent, real-time reconfiguration. These architectures are new to the airlines, and their existing tools and traditional qualitative evaluation techniques are not adequate to evaluate the architectures in terms of meeting the airlines requirements.

In the early 1980s, NASA Langley funded a study by the Boeing Commercial Airplane Co. to comprehensively examine the economic impact of fault-tolerant systems when used on commercial transports. The final report from the study, CR 166043 "Cost and Benefits Optimization Model for Fault-Tolerant Aircraft Electronic Systems," is the only known non-proprietary information on the architecture evaluation issues the airlines now face. NASA funding constraints precluded further study so the models developed in the report have never been reduced to practice.

Consequently, today the airlines have a major need for an operational and economic performance assessment tool for fault-tolerant, flight-critical systems. The most logical starting point for developing the tool is to resume the earlier Langley-sponsored work. By building on this earlier work, I believe the tool could be developed with very modest resources and, furthermore, it could be available relatively quickly.

Observations on NASA Langley/ISD Projects

John Reed
Federal Aviation Administration Technical Center

The NASA Langley advanced flight control systems basic/fundamental research technology projects in the past, and those currently underway, have been beyond reproach. Those efforts in the forefront of civil/military industry needs are:

- software/hardware reliability assessment
- software/hardware fault-tolerant computer concept development
- verification and validation tools, techniques, and methodologies
- solid state device physics and upset studies
- lightning characterization and modeling
- emulation/simulation in systems design, verification and validation, and testing
- AIRLAB

It is obvious to the technologists and users that the U. S. has lost ground in the commercial aircraft business, and possibly is on the edge of loss of preeminence in military aircraft design and operations. With the advent of Airbus Industrie A-320/330/340 series of aircraft/systems technology, the U.S. aviation industry is losing the competitive edge in the market place. The far-sighted Airbus consortium technology advancement application, state(s) funding, and unique and innovative financing arrangements, plus the American dollar exchange rate, have pushed the airlines into considering options other than purchasing Boeing, Douglas, etc.

Why then has not the US aviation industry made the same innovative leap into the world of users/purchasers who want high technology aircraft? Is it the liability problems or technical risks associated with advanced software-based digital Fly-by-wire/Fly-by-light flight control systems...or the concern that the FAA would never certify such an aircraft? Costs of developing, testing, and certifying aircraft/systems possibly all contribute to some degree, but they are extremely difficult to quantify.

So, where do we go from here? The Flight-Critical Digital Systems Workshop is a good (hopefully) starting place. The industry may not criticize NASA for its current programs, but possibly won't really constructively criticize due to the "giving away its proprietary hand and/or birth rights," or competitive edge. The results of the workshop should indicate the necessity or priorities which may reorder or reconsider current NASA initiatives.

ACEE-EET, IAPSA, etc., go a long way in industry participation in proof of concept or technology application. With the transition from aluminum to composite airframes, analog to digital, separate subsystem/system design and implementation to the truly complex integrated (i.e., pilot/crew, flight control, structure, and propulsion, etc.) flight systems, it is necessary to consider a government/industry cost sharing effort to accelerate the US resurgence in the aircraft/systems market.

It appears that a super-effort, such as the SST, with appropriate Congressional mandates and funding could go a long way to rectify the delinquency of having the next generation transport aircraft operational in early year 2000. Military technology transfer, NSF and DARPA fundamental research, NASA and industry basic and applied technology development, innovative certification processes, and an all out US supported activity could make it possible for recovery by the year 2000.

Yes, there are major technical challenges (not stumbling blocks) to the integrated Fly-by-wire/Fly-by-light (FBW/FBL) aircraft. "Flight- Critical" alludes to full-time on-line with no failures for continued safe flight and landing. One must produce a good requirements definition and system architecture to perform its intended function. There are many detailed subsets of hardware/software reliability, unique design strategies and methodologies, upset/fault tolerance, functions, verification/validation, flight operations and maintenance that must be added. Analytical models and tools, emulation/simulation techniques, experimental testing, lightning, and EME protection will be a major effort in the reduction of technical risks. Threat models, transfer function knowledge, susceptibility model and test concepts, innovative immune technology development, etc., must be priority efforts.

After the above, one can say, "NASA is doing that required research." With only 4-5% - NASA funding for aeronautical research, and Information

Systems Division (ISD) less than $6M budget, it will be most difficult to mount a major initiative from FY-89, up through the year 2000. Therefore, NASA should view the Workshop output constructively, review its current program efforts, and within its current budget constraints, prioritize/modify its program direction.
May I now impart some of "J. Reed's thoughts and observations:"

Requirements are:

- Primary "Flight Critical" Digital Flight Control System shall:
  - perform its intended function.
  - be available for the required continued safe flight and landing.
  - in a situation of fault, failure, upset, hiccup, etc., continue to operate its intended functions with no perceptible indications of fault, failure, upset. etc., to the pilot/crew.
- The flight control system and its associated sensors, computers, actuators, displays, power/signal cabling, etc., shall be protected and tested in accordance with the following[4]:
  - be protected and tested in accordance with the FAA rules and regulations, and Advisory Circular AC-20-XX-... "...Lightning Protection of Electrical/Electronic Systems..." and Users Manual DOT-FAA-CT-XX/XX Report (same title).
  - be protected and tested in accordance with the FAA rules and regulations, and Advisory Circular AC-20-XX- "Aircraft Radiated Environment (High Energy RF Fields)", and Users Manual DOT/FAA/CT-XX/XX Report (same title).
  - be protected and tested in accordance with RTCA DO-160C Section 20.0 (HERF), and Section 22.0 (Lightning).

Research needs are: (Complementary to Workshop Session Needs)

- Study, experiment, and test the "upset" phenomena as related to the basic solid state devices:

[4] Some of these documents are not yet officially published.

  - Investigate with manufacturers the characteristics and reliability of their devices.
  - Consider the fundamental, applied research needs in order to design and develop a microprocessor device/module which will be immune to the upset phenomena. (This recommendation assumes that the manufacturers do not support this research activity.)
  - Experiment and test the device, generic subsystem/system applications under lightning, EME, transient, etc., conditions.
  - Apply this technology in a generic flight control systems, design, development, and test (ground/flight) program.

- Conduct a full-scale commercial aircraft, i.e., B-747/767, MD-80, Starship, etc., lightning and HERF test activity.
  - Test to determine transfer function on an aluminum and composite aircraft.
  - Measure internal environment on cabling, subsystem/systems in an aircraft non-operational/operational condition.
  - In order to establish margins of safety:
    - Test to level where systems(s) are upset.
    - Test to level where system(s) may be damaged.
  - Develop/enhance susceptibility models and tools for design of protection concepts.
  - Based on measurements, tests, modeling, etc., design, develop, and test a generic protected (lightning/EME) flight control system.

- Explore/investigate a technique to acquire real-time HERF data from civil/military flight operations.

- Conduct an investigation and analysis of current operational digital flight control and avionic system experience, reliability, failure data, etc.

- Continue to explore the use of simulation in the verification and validation (v&v) and certification process.

- Conduct investigations into the revalidation of flight-critical systems after removal/replacement of Line Replaceable Units, i.e., systems performance, lightning/EME protection integrity, etc.
- Conduct investigations into on board systems and equipment health monitoring and reporting concepts.
- DoD and/or NASA satellite measurements and identification of world-wide HERF levels, i.e., NASA Lightning observations.
- Investigations and studies on similar vs dissimilar flight control systems design concepts, i.e., design, functional, implementation, etc.
- Conduct comprehensive investigations of pilot/crew experience with current flight operations using digital flight control and avionic systems.
  - Based on these investigations:
    - conduct a systems design study which uses the pilot/crew integration inputs.
    - with a generic flight control system, conduct comprehensive cockpit simulator investigations to verify pilot/crew inputs.

Basically, advanced designs must consider a truly integrated set of requirements from all disciplines and parties, not just flight control, propulsion, aerodynamics, structural, etc.

APPENDIX E

ASSESSMENT TEAM REPORT SUMMARY VIEWGRAPHS

NASA LANGLEY FLIGHT-CRITICAL SYSTEMS RESEARCH PROGRAMS

ASSESSMENT TEAM REPORT
as of
May 1989

Summary Viewgraphs

OBJECTIVES

- Review of the NASA Langley flight-critical systems research program
  - Attendance at a one-day briefing
  - Review of representative research publications
- Participate at the Flight-Critical Digital Systems Technology Workshop held at NASA Langley on December 13-15, 1988
- Assess research program coverage of industry needs
- Summarize and report on recommendations

ASSESSMENT TEAM MEMBERS

Dr. Daniel P. Siewiorek, Chairman
Carnegie-Mellon University

Mr. Cary R. Spitzer, NASA Representative
NASA Langley Research Center

Dr. Eliezer G. Gai
The Charles Stark Draper Laboratory, Inc.

Mr. Herman Schmid
General Electric Co.

Ms. Janet R. Dunham, Coordinator
Research Triangle Institute

Mr. Greg Chisholm
Argonne National Laboratory

Mr. John E. Reed
Mr. Peter J. Saraceni
FAA Technical Center

Dr. Anthony S. Wojcik
Michigan State University

ASSESSMENT TEAM BRIEFING AGENDA

December 6, 1988, Building 1220, Room 110

8:30 a.m.	Welcome	Creedon
8:45 a.m.	Introduction	Meissner
9:15 a.m.	AIPS	Pitts
9:45 a.m.	IAPSA	Palumbo
10:15 a.m.	Fault-Tolerant Software	Eckhardt
10:45 a.m.	Software Reliability	Finelli
11:15 a.m.	Redundant VHSIC	Hayes
11:45 a.m.	Lunch	
1:00 p.m.	Mathematical Verification	Butler
1:45 p.m.	Reliability Modeling by Path Analysis	Butler
2:15 p.m.	System Upset	Belcastro
2:45 p.m.	Reliability Modeling by Behavioral Decomposition	Bavuso
3:30 p.m.	Fault Simulation, G-GLOSS	Bavuso
4:00 p.m.	Assessment Team Meeting	

FLIGHT-CRITICAL DIGITAL SYSTEMS TECHNOLOGY WORKSHOP AGENDA

December 13, 1988

9:00 a.m. — 12:00 noon: Opening Session (Overview Talks)

9:00	Dr. J.F. Creedon, NASA Langley Research Center
9:30	Dr. Thomas B. Cunningham, Honeywell Systems Research Center
10:00	Dr. Carl S. Droste, General Dynamics
10:30	Mr. Jim Treacy, Federal Aviation Administration
11:00	Mr. Larry J. Yount and Mr. Richard F. Hess Honeywell Commercial Flight Systems
11:30	Mr. Richard S. Ullman, ITT Defense Technology Corporation

1:00 p.m. — 5:00 p.m.: First Parallel Working Groups Session

- Requirements for Flight-Critical Digital Systems — Aeronautical
- Requirements for Flight-Critical Digital Systems — Space
- System Design for Validation
- Failure Modes
- System Modeling
- Reliable Software
- Flight Test

FLIGHT-CRITICAL DIGITAL SYSTEMS TECHNOLOGY WORKSHOP AGENDA (Continued)

December 14, 1988

8:30 a.m. — 12:00 noon: Second Parallel Working Group Session

1:00 p.m. — 5:00 p.m.: Third Parallel Working Group Session

December 15, 1988

8:30 a.m.	Chairmen's Reports
12:30 p.m.	Workshop Adjourns

RESEARCH PROGRAM ASSESSMENT

GENERAL COMMENTS

- For over two decades, NASA Langley has been a leader in high-dependability flight-critical systems research
- The pioneering work conducted has had far reaching impact (e.g., SIFT and FTMP)
- The research program has been appropriately broad based
- Effective use has been made of peer reviews and external panels in maintaining research quality

GENERAL COMMENTS
(Continued)

- Staff is spread thin among the current research programs
- Technology transfer activities are critical and not completely effective (e.g., modeling tools)
- Additional resources are required to make technology transfer more effective

INDUSTRY NEEDS

Research Topic	Industry Need
Validation	1.1 System Stress Testing
	1.2 Validated Hierarchical Integrated Tool Set
Assessment	2.1 Modeling Tools
	2.2 New Algorithms
	2.3 System Design Figures of Merit
Design (hardware and software)	3.1 Cost Trade-off and Effectiveness of Design Methodologies and Fault Tolerance Concepts
	3.2 Verifiable Building Blocks
	3.3 Formal Verification
	3.4 Life Cycle Considerations During Design
EM Upset	4.1 Threat Modeling, Propagation Analysis and Testing
Data Collection	5.1 In-service Experience
Maintenance	6.1 Modeling, Design for Maintenance after Certification

HIGHEST PRIORITY OF INDUSTRY NEEDS
(Assessment Team Consensus)

Priority	Industry Needs
1	1.2 Validated hierarchical integrated tool set
2	3.1 Cost trade-off and effectiveness of design
3	2.1 Modeling - ease of use, verification, cost/performance
3	4.1 Threat modeling, propagation analysis & testing
4	5.1 In-service experience
5	2.2 New algorithms
5	3.2 Verifiable building blocks

INDUSTRY NEEDS VS. RESEARCH PROGRAM

F Full coverage; i.e., aware of all approaches proposed during workshop

P Partial coverage; i.e., only working on part of the problems identified by the workshop

? Insufficient information for determining coverage

INDUSTRY NEEDS VS. RESEARCH PROGRAM
(Continued)

On-going/In-house	Industry Needs					
IN-HOUSE RESEARCH PROGRAMS	VALIDATION	ASSESS-MENT	DATA/ DESIGN	EM	COLLEC-TION	MAINTE-NANCE
Validation						
Mathematical Verification			3.3F			
Knowledge-Based Systems		2.2?				
Advanced Information Processing System (AIPS)	1.1P		3.2P			
Integrated Airframe Propulsion System Architecture (IAPSA)			3.1P			
Assessment						
Reliability Analysis Tools		2.1P				
Fault Simulation		2.1F				
SW Reliability & FT						
Software Reliability			3.1P			
FT S/W			3.1P			
EM Upset						
Upset Research at Langley				4.1P		

OBSERVATIONS

- Within the scope of the activities conducted, the research program is very sound and could benefit from additional dollars:
  - All tasks under the current research program are at least partially addressing the industry needs
  - Except for Industry Need 5.1, In-service Experience, the research program is addressing (with varying degrees of coverage) the higher priority industry needs identified
  - Due to funding limitations there are significant number of industry needs either not being covered or not being covered adequately
  - The current program is front-end loaded in terms of the life cycle

KEY RECOMMENDATIONS

- Program resources should be substantially expanded to give adequate coverage to the research and extended to the industry needs identified
- The current program needs to be extended to include research development in operations and maintenance
- Additional research tasks should be initiated to meet the five higher priority industry needs specified
- Focus the research program by selecting an actual hardware and software system that is under development as a vehicle for an ongoing evaluation of the emerging technology

RECOMMENDATIONS FOR ADDITIONAL RESEARCH TASKS

- The development of a validated hierarchical integrated tool set that can be used to address issues related to life-cycle validation
- The conduct of cost-tradeoff and effectiveness studies of design methodologies and fault tolerance concepts
- The development and verification of easy-to-use modeling tools that address reliability, performance, coverage, and cost
- The conduct of threat modeling, and propagation analysis and testing. In particular, develop design verification criteria for Electromagnetic Environment(EME)and High Energy Radio Frequency (HERF) related threats.
- The compilation and analysis of in-service data

NASA
National Aeronautics and Space Administration

Report Documentation Page

1. Report No. NASA CR-181850	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle
Assessment Team Report on Flight-Critical Systems Research at NASA Langley Research Center

5. Report Date
August 1989

6. Performing Organization Code

7. Author(s)
Daniel P. Siewiorek and Janet R. Dunham, Compilers

8. Performing Organization Report No.

10. Work Unit No.
505-66-21-03

9. Performing Organization Name and Address
Research Triangle Institute
Center for Digital Systems Research
Post Office Box 12194
Research Triangle Park, NC 27709-2194

11. Contract or Grant No.
NAS1-17964, Task 29

13. Type of Report and Period Covered
Contractor Report

12. Sponsoring Agency Name and Address
National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23665-5225

14. Sponsoring Agency Code

15. Supplementary Notes Assessment Team Members: Daniel P. Siewiorek, Chairman; Cary R. Spitzer, NASA Representative; Janet R. Dunham, Coordinator; Greg Chisholm, Eliezer G. Gai, John E. Reed, Peter J. Saraceni, Herman Schmid, and Anthony S. Wojcik. Langley Technical Monitor: Charles W. Meissner, Jr.
Daniel P. Siewiorek: Carnegie-Mellon University, Pittsburgh, Pennsylvania
Janet R. Dunham: Research Triangle Institute, Research Triangle Park, NC

16. Abstract

This publication was written by a 9-member Assessment Team to assess the quality, coverage, and distribution of effort of the flight-critical systems research program at NASA Langley Research Center. The Assessment Team, formed in November 1988, had two primary sources of information: (1) review of the research program by attending a one-day briefing at NASA Langley and reviewing representative research publications and (2) participation at the Flight-Critical Digital Systems Technology Workshop held at NASA Langley on December 13-15, 1988. Within the scope of the Assessment Team's review, the research program was found to be very sound. All tasks under the current research program were at least partially addressing the industry needs. General recommendations made were to expand the program resources to provide additional coverage of high priority industry needs, including operations and maintenance, and to focus the program on an actual hardware and software system that is under development.

17. Key Words (Suggested by Author(s)) Flight-critical research; Validated hierarchical integrated tool set; Design methodologies; Fault tolerance concepts; Development and verification; Electromagnetic Environment (EME); High Energy Radio Frequency (HERF); In-service data.

18. Distribution Statement
[redacted]
Subject Category 05

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of pages 69	22. Price